Virtual noiseless amplification and Gaussian post-selection in continuous-variable quantum key distribution

Jaromír Fiurášek[1] and Nicolas J. Cerf[2]

[1]*Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2]*QuIC, Ecole Polytechnique de Bruxelles, Université Libre de Bruxelles, 1050 Brussels, Belgium*

The noiseless amplification or attenuation are two heralded filtering operations that enable respectively to increase or decrease the mean field of any quantum state of light with no added noise, at the cost of a small success probability. We show that inserting such noiseless operations in a transmission line improves the performance of continuous-variable quantum key distribution over this line. Remarkably, these noiseless operations do not need to be physically implemented but can simply be simulated in the data post-processing stage. Hence, *virtual* noiseless amplification or attenuation amounts to perform a Gaussian post-selection, which enhances the secure range or tolerable excess noise while keeping the benefits of Gaussian security proofs.

Continuous-variable quantum key distribution (CV QKD) based on Gaussian states and homodyne or heterodyne detection can achieve very high secret key rates, see e.g. [1] for a review. Moreover, its practical implementation does not require single-photon detectors and the system can be made compatible with telecom optical networks [2]. However, although theory predicts that a secure key can be generated for a pure loss channel over an arbitrary large distance [3], the practical range of CV QKD is currently limited to several tens of kilometers by noise and imperfect classical data processing [4, 5].

In contrast to classical optical networks, losses in quantum communication channels cannot be compensated by usual phase-insensitive amplifiers as the latter inevitably add noise [6], making the channel insecure. Recently, however, the concept of heralded noiseless quantum amplification has emerged as a novel tool [7], which enables one to probabilistically increase the amplitude of a coherent state without adding any extra noise, $|\alpha\rangle \rightarrow |g\alpha\rangle$ with gain $g > 1$. Of course, a natural question arises whether this noiseless amplifier may improve the performance of QKD, especially enhance its secure range. In ref. [8], it was indeed argued that (a double version of) the noiseless amplifier can be beneficial for device-independent quantum cryptography with single photons.

Here, we investigate this question in more general terms. We start from the observation that any physical realization of the noiseless amplifier turns out to be very demanding. Even the proof-of-principle experimental noiseless amplification of weak coherent states requires state-of-the art technology, such as single-photon addition and subtraction, or an auxiliary source of single photons and multiphoton interference [9–13]. Moreover, the actual success rate of these experiments is much lower than the theoretical predictions due to various experimental limitations, and the transformation can furthermore only be implemented approximately. Such an approach seems rather impractical in the context of CV QKD where the system should be reasonably simple and robust to allow for field deployment.

In this paper, we show that the physical implementation of the noiseless amplifier can be substituted with a suitable data processing, so that the amplification is performed only virtually. Just like *virtual* entanglement is used to analyze the security of prepare-and-measure protocols [14], it appears that *virtual* noiseless amplification may simulate the associated quantum filter and be beneficial to CV QKD. We also turn our attention to a dual quantum filter called noiseless attenuation, which is analogous to noiseless amplification but with a gain lower than one [15]. It probabilistically transforms $|\alpha\rangle \rightarrow |\nu\alpha\rangle$ with gain $\nu < 1$, so it is akin to a beam splitter but it effects the same decrease of the mean amplitude for any state with no noise. Noiseless attenuation can also be faithfully emulated by classical postprocessing of the experimental data with a reasonable overhead (as we shall see, noiseless amplification can in principle be emulated arbitrarily well, but an exact emulation is in contrast only possible in the limit of a low success probability due to heavy rejection).

We shall demonstrate that virtual noiseless amplification or attenuation can extend the range of CV QKD over noisy channels. A simple picture, which provides a good intuition of this effect though it is not rigorous, is as follows. The emitter (Alice) preprocesses her signal states by noiselessly attenuating them, thereby making them strongly indistinguishable to an eavesdropper (Eve). At the other end of the line, the receiver (Bob) revives the signal states by noiselessly amplifying them. Since the two quantum filters are Gaussian (trace-decreasing) operations, the pre- and post-selected data appear as if they emerged from a deterministic Gaussian protocol; hence, the security proofs based on the optimality of Gaussian attacks hold [16–18]. Somehow, Eve cannot bias the pre- and post-selection filters, and the above "compaction" of the signal states in the channel can only be detrimental to her. In practice, the pre-selection is not needed (it amounts to reducing the modulation variance), while the post-selection associated with noiseless amplification can be applied virtually on the experimental data.
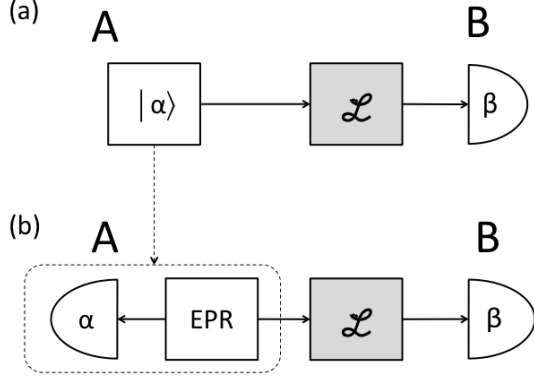
FIG. 1: (a) Prepare-and-measure CV QKD protocol with coherent states and heterodyne detection. (b) Equivalent virtual entanglement-based protocol, with heterodyne detection on both sides.
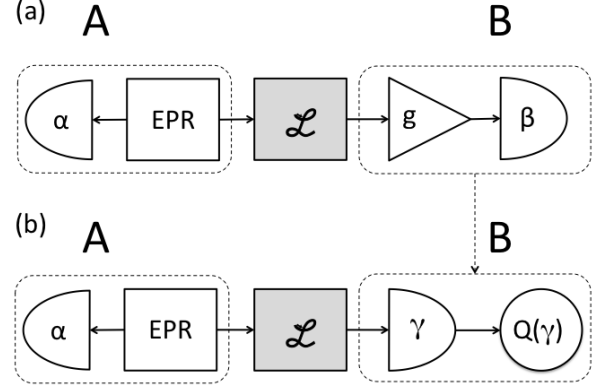

FIG. 2: (a) CV QKD with coherent states and heterodyne detection augmented with noiseless amplification of the received signal. (b) Equivalent protocol where noiseless amplification is emulated by post-processing Bob's measurement data.

CV QKD protocols.—Gaussian protocols, to which we restrict here, are based on the Gaussian modulation of Gaussian (coherent or squeezed) states of light and Gaussian (homodyne or heterodyne) measurements, which gives four possibilities. In the first two protocols, Bob performs homodyne detection, measuring at random the x or p quadrature, while Alice emits a Gaussian-modulated coherent [19] or squeezed [20] state. In the next two, Bob performs heterodyne detection, measuring the x and p quadratures simultaneously, while Alice emits again a coherent [21] or squeezed [22] state. Note the existence of a fifth protocol, where Alice sends (mixed) thermal states instead of pure states [23].

In what follows, we focus on the most symmetric protocol [21], where Alice emits coherent states $|\alpha\rangle$ and Bob projects onto coherent states $|\beta\rangle$ (heterodyne detection), as illustrated in Fig. 1(a). Alice draws a complex amplitude α from a bivariate Gaussian distribution of variance V, and sends $|\alpha\rangle$ to Bob through a quantum channel $\mathcal{L}$ which is controlled by Eve. Then, Bob makes a projective measurement onto coherent states and obtains the outcome β. After N repetitions of these steps, Alice and Bob extract a secret key from the accumulated classical data. From Eve's point of view, this prepare-and-measure protocol is indistinguishable from an entanglement-based scheme where Alice prepares an entangled two-mode squeezed vacuum state

$$|\Psi_{\mathrm{EPR}}\rangle = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n |n,n\rangle \qquad (1)$$

with $\lambda^2 = 2V/(2V+1)$, and performs heterodyne measurement on one mode, see Fig. 1(b).

This virtual entanglement picture [14] is very useful for analyzing the security and understanding the benefit of noiseless amplification. Suppose that $\mathcal{L}$ is a pure loss channel with transmittance T. As shown in ref. [24], an entangled state (1) can be faithfully distributed over $\mathcal{L}$ if Alice sends one mode of a weakly entangled state ($\lambda \ll 1$) to Bob, who noiselessly amplifies his mode. In the considered CV QKD protocol, this would correspond to weak modulation on Alice's side ($V \ll 1$) combined with noiseless amplification on Bob's side, see Fig. 2(a).

Virtual noiseless amplification.—The noiseless amplifier is described by the non-unitary operator $g^{\hat{n}}$, where $\hat{n}$ denotes the photon number operator. Although it is probabilistic, this filter is Gaussian in the sense that it converts a Gaussian state between Alice and Bob in the virtual entanglement picture into another Gaussian state. Forgetting about the modulation variance V, this can be viewed as effectively converting the Gaussian channel $\mathcal{L}$ into another Gaussian channel with presumably higher associated performances. Moreover, we can recycle all security proofs and corresponding secret key rates that have be obtained using the Gaussian formalism [16–18].

Unfortunately, $g^{\hat{n}}$ is an unbounded operator for $g > 1$, so it cannot be implemented exactly, and, furthermore, its optical implementation is very challenging. Remarkably, these obstacles can be overcome by emulating the noiseless amplifier, which is possible as it is immediately followed by heterodyne measurement. Note that we can consider the noiseless amplifier $g^{\hat{n}}$ at the output of channel $\mathcal{L}$ to be part of the detection process, see Fig. 2(a). Denoting by $\hat{\rho}$ the mixed state at the output of $\mathcal{L}$, Bob obtains (after amplification) the measurement outcome β with relative probability

$$P_g(\beta) = \frac{1}{\pi} \langle\beta|g^{\hat{n}} \hat{\rho} \, g^{\hat{n}}|\beta\rangle. \qquad (2)$$

Using the identity $g^{\hat{n}}|\beta\rangle = e^{(g^2-1)|\beta|^2/2}|g\beta\rangle$, we can write

$$P_g(\beta) = \frac{1}{\pi} \, e^{(g^2-1)|\beta|^2} \langle g\beta|\hat{\rho}|g\beta\rangle. \qquad (3)$$

If Bob directly measures $\hat{\rho}$ without prior amplification, he gets the outcome γ with probability $P(\gamma) = \frac{1}{\pi}\langle\gamma|\hat{\rho}|\gamma\rangle$. By comparing this probability with Eq. (3), we conclude that Bob can emulate the noiseless amplificater by properly rescaling each measurement outcome γ as $\beta = \gamma/g$, while assigning to it a relative weight $Q(\gamma) = e^{(1-g^{-2})|\gamma|^2}$, see Fig. 2(b).

This relative weight can be simulated by post-selection, accepting each data γ with a probability $P_{\rm acc}(\gamma)$ that is proportional to $Q(\gamma)$. A difficulty arises here because $Q(\gamma)$ diverges for large $|\gamma|$, which translates the impossibility of implementing a perfect noiseless amplifier. If Alice's modulation V is weak enough, $P(\gamma)$ could be sufficiently narrow so that $\lim_{|\gamma|\to\infty} P(\gamma)Q(\gamma) = 0$. Then, for a finite number N of data points γ_j, one can accept each one with probability

$$P_{\rm acc}(\gamma) = e^{(1-g^{-2})(|\gamma|^2-|\gamma_M|^2)} \leq 1. \qquad (4)$$

where $|\gamma_M| = \max_j |\gamma_j|$. As derived in the Appendix, the number of accepted data points $N_{\rm acc}$ grows sublinearly with the size N, so unfortunately the rejection rate increases with N and the procedure becomes rather inefficient. Alternatively, one can fix $|\gamma_M|$ independently of N. For instance, if $P(\gamma)Q(\gamma)$ is expected to exhibit a distribution with variance V_γ, then one can choose $|\gamma_M|$ as a multiple of $\sqrt{V_\gamma}$ (say, 10 standard deviations) and set $P_{\rm acc}(\gamma) = 1$ if $|\gamma| > |\gamma_M|$. Assuming a Gaussian distribution of variance V_B for Bob's measurement outcomes γ, we show in the Appendix that $N_{\rm acc}$ scales linearly with N in this case, namely

$$\frac{N_{\rm acc}}{N} \approx \frac{g^2}{g^2 + 2V_B(1-g^2)} \left[e^{-(1-g^{-2})|\gamma_M|^2} - e^{-\frac{|\gamma_M|^2}{2V_B}} \right] \qquad (5)$$

Note that this only works if $2V_B < g^2/(g^2 - 1)$. Given its linear scaling, this second method is more practical than the first one although the data processing does not emulate the exact Gaussian filter because of the finite cut-off, which might complicate the security analysis.

Virtual noiseless attenuation.—In view of these difficulties, we also consider a reverse situation where the noiseless amplifier is on Alice's side (replaced, in fact, by a larger V) while the noiseless attenuator is on Bob's side (replaced by its virtualization). The noiseless attenuation $\nu^{\hat{n}}$ with $\nu < 1$ is a physical operation, which can be implemented by sending the state through a beam splitter of transmittance ν^2 and projecting the auxiliary output port of the beam splitter onto vacuum. Although the efficiency of common single-photon detectors is too low to implement this latter projection with high fidelity, one can faithfully emulate noiseless attenuation with an acceptable overhead. The principle is the same as before. Denoting by $\hat{\rho}$ the state emerging from $\mathcal{L}$, the relative probability of the measurement outcome β after attenuation can be expressed as

$$P_\nu(\beta) = \frac{1}{\pi}\langle\beta|\nu^{\hat{n}}\hat{\rho}\,\nu^{\hat{n}}|\beta\rangle = \frac{1}{\pi}e^{-(1-\nu^2)|\beta|^2}\langle\nu\beta|\hat{\rho}|\nu\beta\rangle. \qquad (6)$$
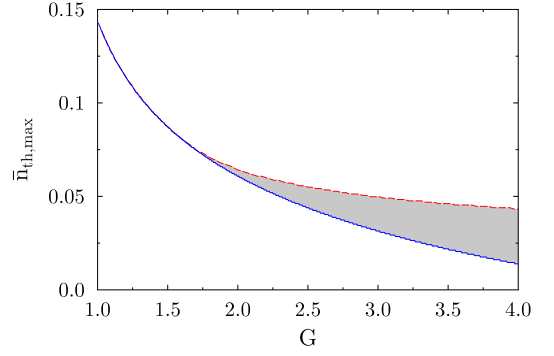

FIG. 3: CV QKD over an amplifying channel with gain G and excess thermal noise $\bar{n}_{\rm th}$. The maximum allowed noise $\bar{n}_{\rm th,max}$ decreases for increasing G. A secret key can be generated if $\bar{n}_{\rm th} < \bar{n}_{\rm th,max}$, shown with the blue solid line (standard protocol) or red dashed line (protocol augmented with virtual noiseless attenuation). The grey area indicates the class of channels for which no key can be generated without virtual noiseless attenuation. We optimize over Alice's modulation variance V and Bob's attenuation ν, and assume $\eta = 0.9$.

Since $\nu < 1$, we have $e^{-(1-\nu^2)|\beta|^2} < 1$, hence no divergence problem. Therefore, we can emulate noiseless attenuation by rescaling the measurement outcome γ as $\beta = \gamma/\nu$ and accepting the data point with probability $Q(\gamma) = e^{-(\nu^{-2}-1)|\gamma|^2} < 1$. In this way, we post-select a subset of the original data that corresponds to a protocol where the signal would be noiselessly attenuated before heterodyne detection. As illustrated in the Appendix, this emulation is efficient in the sense that the number of accepted data points is proportional to the original size,

$$\frac{N_{\rm acc}}{N} = \frac{\nu^2}{\nu^2 + 2V_B(1-\nu^2)}, \qquad (7)$$

The noiseless attenuation is a trace-decreasing Gaussian completely-positive map, so it preserves the Gaussian form of the entangled state between Alice and Bob. Therefore, the security results on deterministic CV QKD protocols with Gaussian modulated coherent states can be applied to this protocol with virtual noiseless attenuation inserted on Bob's side (without the heavy-rejection problem of virtual noiseless amplification).

CV QKD with Gaussian post-selection.—Exploiting that the (Gaussian) quantum filter effected by the noiseless amplifier or attenuator can be emulated during the post-processing stage, we now investigate the benefit of the resulting Gaussian post-selection for CV QKD. As an instructive example, we first consider virtual noiseless attenuation at the output of a Gaussian amplifying channel with excess noise [25], see Fig. 3. In the Heisenberg picture, this channel is described by a linear transformation of the annihilation and creation operators,

$$\hat{a}_{\rm out} = \sqrt{G}\hat{a}_{\rm in} + \sqrt{G-1}\,\hat{c}^\dagger, \qquad (8)$$

where $\hat{a}$ and $\hat{c}$ denote the annihilation operators of the signal and ancilla modes, respectively, and G is the chan-
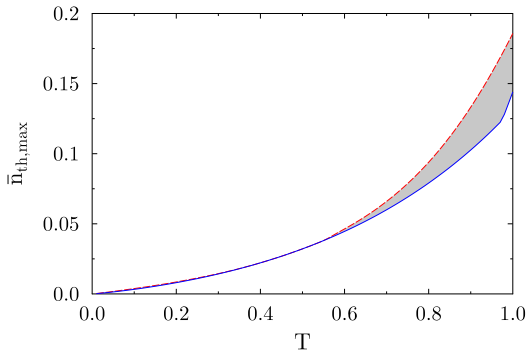
FIG. 4: CV QKD over a lossy channel with transmittance T and excess thermal noise $\bar{n}_{\mathrm{th}}$. The maximum allowed noise $\bar{n}_{\mathrm{th,max}}$ decreases for decreasing T. A secret key can be generated if $\bar{n}_{\mathrm{th}} < \bar{n}_{\mathrm{th,max}}$, shown with the blue solid line (standard protocol) or red dashed line (protocol augmented with virtual noiseless amplification). The grey area indicates the class of channels for which no key can be generated without virtual noiseless amplification. We optimize over Alice's modulation variance V and Bob's amplification g, and assume $\eta = 0.9$.

nel gain. This channel is not quantum-noise limited, which is modeled by assuming that the ancilla mode is initially prepared in a thermal state with mean photon number $\langle c^{\dagger}c \rangle = \bar{n}_{\mathrm{th}}/(G-1)$, where $\bar{n}_{\mathrm{th}}$ is the mean number of excess thermal photons injected into the signal mode. Sending one part of the entangled state (1) through this channel yields a mixed two-mode Gaussian state with covariance matrix

$$\gamma_{AB} = \begin{pmatrix} a\,I & c\,\sigma_z \\ c\,\sigma_z & b\,I \end{pmatrix}, \qquad (9)$$

where $a = \cosh(2r)$, $b = G\cosh(2r) + G - 1 + 2\bar{n}_{\mathrm{th}}$, $c = \sqrt{G}\sinh(2r)$, and $r = \tanh^{-1}(\lambda)$. Here, I stands for the 2×2 identity matrix and σ_z stands for the third Pauli matrix. The covariance matrix of the Gaussian state obtained conditionally on the success of $\nu^{\hat{n}}$ (or $g^{\hat{n}}$) can be conveniently calculated by exploring a connection between covariance matrix elements and density matrix elements in Fock basis [26], see Appendix. The secret key rate against collective attacks is calculated according to

$$K = \max(\eta I_{AB} - \chi_{AE},\, \eta I_{AB} - \chi_{BE}), \qquad (10)$$

where the first (second) term corresponds to direct (reverse) reconciliation, so we choose the protocol that yields the higher secret key rate (η is the reconciliation efficiency). Here, I_{AB} is Shannon mutual information between Alice and Bob, while χ_{AE} (χ_{BE}) is the Holevo quantity between Alice and Eve (Bob and Eve). All these quantities can be calculated using standard methods (see Appendix) since we know the post-selected virtual Gaussian entangled state shared by Alice and Bob. In Fig. 3, we show the dependence of the maximum allowed thermal noise $\bar{n}_{\mathrm{th,max}}$ on the channel gain G. It appears that for sufficiently high G, the inclusion of virtual noiseless

attenuation is advantageous as a secret key can be generated for a higher level of thermal noise.

We have also performed similar calculations for a lossy channel with transmittance T and excess noise $\bar{n}_{\mathrm{th}}$, see Appendix. Unexpectedly, noiseless attenuation also helps here if T is not too small, although the effect is tiny. We do not plot it here as the effect is similar but much more pronounced by inserting noiseless amplification instead of attenuation on Bob's side. As shown in Fig. 4, the protocol tolerates more thermal noise $\bar{n}_{\mathrm{th}}$ for a fixed T when it is augmented with virtual noiseless amplification. Note that we have neglected the slight non-Gaussianity induced by the post-selection cutoff when calculating the secret key rates. We have also assumed a realistic value $\eta = 0.9$ for the efficiency of the classical data reconciliation [4, 5]. The advantage of virtual noiseless amplification would be even stronger for $\eta \to 1$, but this is a rather unrealistic limit as error correction is a highly challenging task in practical CV QKD [2].

Conclusion.—We have demonstrated the improved performance (enhanced secure range or tolerable excess noise) of a CV QKD protocol with coherent states, heterodyne detection, and *virtual* noiseless amplification or attenuation. The latter quantum filters do not need to be physically implemented, which would be experimentally quite challenging, but may be simulated by classical post-processing (Gaussian post-selection) of the measured data, making this proposal immediately applicable. Furthermore, since the above quantum filters are Gaussian, the post-selected data can be treated as emerging from an effective Gaussian protocol and the security proofs based on Gaussian extremality still hold.

One may also consider virtual operations in protocols where Bob performs homodyne detection. A noiseless attenuation followed by the projection onto squeezed displaced states can be interpreted as a projection onto squeezed displaced state with lower squeezing and rescaled displacements. Thus, to simulate noiseless attenuation, we would need to change the detection scheme so that it performs projections onto finitely squeezed states. This could be achieved by employing an eight-port homodyne detection with unbalanced central beam splitter, such that the amplitude and phase quadratures of the state are measured with different precision. In view of all this, we anticipate that Gaussian post-selection could be a tool of practical importance in CV QKD.

Note: In the course of completion of this work, the importance of noiseless amplification in CV QKD has been independently demonstrated in [27] and [28].

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[3] F. Grosshans, G. Van Assche, J. Wenger R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[4] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[5] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Allaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express (in press); arXiv:1201.3744

[6] C. M. Caves, Phys. Rev. D **26**, 1817-1839 (1982).

[7] T.C. Ralph and A.P. Lund, in *Quantum Communication Measurement and Computing*, Proceedings of 9th International Conference, Ed. A. Lvovsky, 155-160 (AIP, New York 2009); arXiv:0809.0326.

[8] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[9] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nature Phot. **4**, 316-319 (2010).

[10] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[11] M. A. Usuga, C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nature Phys. **6**, 767-771 (2010).

[12] A. Zavatta, J. Fiurášek, and M. Bellini, Nature Phot. **5**, 52-56 (2011).

[13] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, arXiv:1203.3396.

[14] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[15] M. Mičuda, I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek, submitted.

[16] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).

[17] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[18] R. García-Patrón and N.J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[19] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[20] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).

[21] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, Phys. Rev. Lett. **93**, 170504 (2004); S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[22] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[23] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[24] T. C. Ralph, Phys. Rev. A **84**, 022339 (2011).

[25] R. Filip, Phys. Rev. A **77**, 032347 (2008).

[26] J. Eisert, D.E. Browne, S. Scheel, M.B. Plenio, Annals of Physics (NY) **311**, 431 (2004).

[27] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, 9th workshop on continuous-variable quantum information processing, Frederiksdal, April 27-30, 2012; arXiv:1205.0959.

[28] T. C. Ralph *et al.*, 9th workshop on continuous-variable quantum information processing, Frederiksdal, April 27-30, 2012.

Appendix

1. Gaussian post-selection equivalent to the noiseless amplification

The heralded noiseless amplifier corresponds to an (un-bounded) filtration operator $g^{\hat{n}}$ in Fock space. If it is immediately followed by heterodyne measurement, we have shown that it can be replaced by an appropriate post-processing of the measured data. One must rescale each measurement outcome γ as $\beta = \gamma/g$ and assign a relative weight $Q(\gamma) = e^{(1-g^{-2})|\gamma|^2}$ to it. The unboundedness of the quantum filter translates into the fact that $Q(\gamma)$ diverges for large $|\gamma|$, which makes it difficult to devise a good post-selection procedure. A first possibility is to accept each data point γ with probability $P_{\mathrm{acc}}(\gamma) = e^{(1-g^{-2})(|\gamma|^2-|\gamma_M|^2)} \leq 1$, where $|\gamma_M|$ is the maximum value of $|\gamma|$ of the set of size N. Then, numerical simulations suggest that assuming Gaussian distribution for Bob's measurement outcomes

$$P(\gamma) = \frac{1}{2\pi V_B} e^{-\frac{|\gamma|^2}{2V_B}}, \qquad (A.1)$$

the number of accepted data points N_{acc} grows with N. However, the scaling is only sublinear, $N_{\mathrm{acc}} = N^{\kappa}$ where $\kappa < 1$, see Fig. 5. This implies $\lim_{N\to\infty} N_{\mathrm{acc}}/N = 0$ and the procedure becomes inefficient for large N.

A second possibility is to choose a large fixed value for $|\gamma_M|$ and set $P_{\mathrm{acc}}(\gamma) = 1$ if $|\gamma| > |\gamma_M|$. The number of data points N_{acc} preserved after filtering is then lower
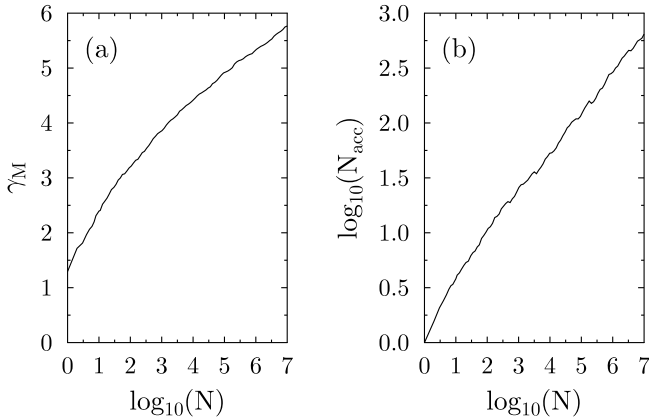

FIG. 5: Virtual noiseless amplification. (a) Dependence of Bob's maximum measurement outcome $|\gamma_M|$ on the number of measurements N. (b) Number of measurement outcomes N_{acc} preserved after filtration is plotted as a function of N. This latter dependence can be approximately described by a power law $N_{\mathrm{acc}} \propto N^{\kappa}$ with $\kappa \approx 0.38$. The graphs were obtained assuming $V_B = 1$ and $g^2 = 1.5$ and the curves represent averages over 100 independent simulations of the filtering procedure.

bounded by

$$N \int_0^{2\pi} \int_0^{|\gamma_M|} P(\gamma) P_{\mathrm{acc}}(\gamma) |\gamma| \, \mathrm{d}|\gamma| \, \mathrm{d}\phi, \qquad (A.2)$$

where $\gamma = |\gamma| e^{i\phi}$. For Gaussian distribution (A.1) one recovers a linear scaling of output data points with N,

$$\frac{N_{\mathrm{acc}}}{N} \geq \frac{g^2}{g^2 + 2V_B(1-g^2)} \left[e^{-(1-g^{-2})|\gamma_M|^2} - e^{-\frac{|\gamma_M|^2}{2V_B}} \right].$$

The integral converges and the emulation is possible only if $2(g^2-1)V_B < g^2$. The emulation of the noiseless amplification is much more practical with this second method, but we have to keep in mind that it does not exactly emulate the target Gaussian filtration as the cutoff $|\gamma_M|$ is finite, which might complicate the security analysis.

2. Gaussian post-selection equivalent to the noiseless attenuation

The idea of replacing the actual noiseless amplifier by some appropriate data post-processing can be applied to the noiseless attenuator too. This amounts to rescaling the measurement outcome γ as $\beta = \gamma/\nu$ and accepting the data point with probability $Q(\gamma) = e^{-(\nu^{-2}-1)|\gamma|^2}$. The main difference is that there is no divergence problem here since $Q(\gamma) < 1$. Therefore, the emulation is efficient in the sense that the number of accepted data points is proportional to the original number of data points,

$$\frac{N_{\mathrm{acc}}}{N} = \int_0^{2\pi} \int_0^{\infty} P(\gamma) e^{-(\nu^{-2}-1)|\gamma|^2} |\gamma| \, \mathrm{d}|\gamma| \, \mathrm{d}\phi.$$

In particular, for Gaussian distribution of Bob's outcomes (A.1) we obtain

$$\frac{N_{\mathrm{acc}}}{N} = \frac{\nu^2}{\nu^2 + 2V_B(1-\nu^2)}.$$

3. Evaluation of the covariance matrices

Elements of covariance matrix γ_{AB} of a two-mode state $\hat{\rho}_{AB}$ are defined as $\gamma_{AB,jk} = \langle \Delta\hat{R}_j \Delta\hat{R}_k + \Delta\hat{R}_k \Delta\hat{R}_j \rangle$, where $\Delta\hat{R}_j = \hat{R}_j - \langle\hat{R}_j\rangle$, $\langle\hat{R}_j\rangle = \mathrm{Tr}[\hat{R}_j \hat{\rho}_{AB}]$ and $\hat{\mathbf{R}} = (\hat{x}_A, \hat{p}_A, \hat{x}_B, \hat{p}_B)$ denotes vector of quadrature operators. Note that variances of quadrature operators of vacuum state are equal to $\frac{1}{2}$, hence the covariance matrix of vacuum is equal to the identity matrix.

Let us now consider a CV QKD protocol where Alice prepares two-mode squeezed vacuum state

$$|\Psi_{EPR}\rangle = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n |n,n\rangle_{AB}, \qquad (A.3)$$

whose covariance matrix reads

$$\gamma_{\mathrm{EPR}} = \begin{pmatrix} a & 0 & \sqrt{a^2-1} & 0 \\ 0 & a & 0 & -\sqrt{a^2-1} \\ \sqrt{a^2-1} & 0 & a & 0 \\ 0 & -\sqrt{a^2-1} & 0 & a \end{pmatrix},$$

and $a = (1+\lambda^2)/(1-\lambda^2)$. Alice keeps mode A for heterodyne measurement, while she transmits mode B through the noisy quantum channel $\mathcal{L}$, which can be assumed Gaussian since this is the worst case (optimal collective attack). The covariance matrix changes to

$$\gamma_{AB} = \begin{pmatrix} a & 0 & c & 0 \\ 0 & a & 0 & -c \\ c & 0 & b & 0 \\ 0 & -c & 0 & b \end{pmatrix}, \qquad (A.4)$$

where

$$b = Ta + 1 - T + 2\bar{n}_{\mathrm{th}}, \quad c = \sqrt{T(a^2-1)}, \qquad (A.5)$$

for a lossy channel with transmittance $T \le 1$ and excess thermal noise $\bar{n}_{\mathrm{th}}$, while

$$b = Ga + G - 1 + 2\bar{n}_{\mathrm{th}}, \quad c = \sqrt{G(a^2-1)}, \qquad (A.6)$$

for an amplifying channel with gain $G > 1$ and excess thermal noise $\bar{n}_{\mathrm{th}}$.

We next determine the covariance matrix of the Gaussian state obtained by applying the quantum filter $g^{\hat{n}}$ to Bob's mode. The cases $g > 1$ and $g = \nu < 1$ cover both noiseless amplification and attenuation, respectively. Inspired by [26], we exploit the relationship between elements of the covariance matrix γ_{AB} and elements of the density matrix $\hat{\rho}_{AB}$ in Fock state basis. The Husimi Q-function of the two-mode state can be expressed as

$$Q(\mathbf{R}) = \frac{\sqrt{\det\Gamma_{AB}}}{\pi^2} e^{-\mathbf{R}^T\Gamma_{AB}\mathbf{R}}. \qquad (A.7)$$

where

$$\Gamma_{AB} = (\gamma_{AB} + I)^{-1}, \qquad (A.8)$$

and I denotes the identity matrix. We can write

$$\Gamma_{AB} = \begin{pmatrix} A & 0 & C & 0 \\ 0 & A & 0 & -C \\ C & 0 & B & 0 \\ 0 & -C & 0 & B \end{pmatrix}, \qquad (A.9)$$

where A, B, and C are functions of a, b, c. Since the Husimi Q-function is a generating function of density matrix elements in Fock basis, one can establish a relationship between elements of matrix Γ_{AB} and normalized density matrix elements in Fock basis $\sigma_{jk,lm} = \frac{\rho_{jk,lm}}{\rho_{00,00}}$ [26]. The action of the filter $\hat{\mathbb{1}}_A \otimes g^{\hat{n}_B}$ is particularly simple in Fock basis,

$$\sigma_{jk,lm} \to g^{k+m}\sigma_{jk,lm}. \qquad (A.10)$$

At the same time, the filtration $g^{\hat{n}}$ is a Gaussian operation which preserves the Gaussian shape of Wigner and Husimi function. After a straightforward calculation one finds that the matrix Γ_{AB} of the Gaussian state after filtration reads,

$$\Gamma'_{AB} = \begin{pmatrix} A & 0 & gC & 0 \\ 0 & A & 0 & -gC \\ gC & 0 & g^2(B-\frac{1}{2})+\frac{1}{2} & 0 \\ 0 & -gC & 0 & g^2(B-\frac{1}{2})+\frac{1}{2} \end{pmatrix}. \qquad (A.11)$$

The covariance matrix γ'_{AB} of the filtered state can then be obtained by inverting the relation (A.8),

$$\gamma'_{AB} = (\Gamma'_{AB})^{-1} - I. \qquad (A.12)$$

4. Evaluation of the secret key rates

The protocol where Alice prepares coherent states and Bob performs heterodyne detection is formally equivalent to entanglement-based protocol where Alice prepares two-mode squeezed vacuum, sends one mode to Bob, and both Alice and Bob perform heterodyne detection. In this way, Alice and Bob obtain Gaussian correlated data whose statistics is governed by Husimi Q-function (A.7) and the mutual information between Alice and Bob is given by

$$I_{AB} = \log_2 \frac{(a+1)(b+1)}{(a+1)(b+1)-c^2}. \qquad (A.13)$$

The Holevo quantity χ_{AE} can be expressed as

$$\chi_{AE} = S(\hat{\rho}_{AB}) - \sum_j p_j S(\hat{\rho}_{B,j}), \qquad (A.14)$$

where $S(\hat{\rho})$ denotes von-Neumann entropy of quantum state $\hat{\rho}$ and $\hat{\rho}_{B,j}$ denotes density matrix of Bob's mode conditional on jth measurement outcome of Alice. Note that the expression (A.14) follows from the fact that Eve holds purification of the quantum state shared by Alice and Bob hence the entropies of Eve's states appearing in the original definition of χ_{AE} are equal to the entropies of states of Alice and Bob. If Alice projects onto coherent states, then all states $\hat{\rho}_{B,j}$ are Gaussian, have the same covariance matrix

$$\gamma_B = \begin{pmatrix} b - \frac{c^2}{a+1} & 0 \\ 0 & b - \frac{c^2}{a+1} \end{pmatrix} \qquad (A.15)$$

and differ only in displacements. Therefore all Bob's conditional states have the same entropy S_B and we can write

$$\chi_{AE} = S_{AB} - S_B. \qquad (A.16)$$

The von-Neumann entropies of Gaussian states appearing in the above formula can be calculated as follows,

$$S_{AB} = \sum_{j=1}^{2} \left(\frac{\mu_j+1}{2}\log_2\frac{\mu_j+1}{2} - \frac{\mu_j-1}{2}\log_2\frac{\mu_j-1}{2} \right), \qquad (A.17)$$

where μ_j denote symplectic eigenvalues of the covariance matrix γ_{AB}, and

$$S_B = \frac{\mu+1}{2} \log_2 \frac{\mu+1}{2} - \frac{\mu-1}{2} \log_2 \frac{\mu-1}{2}, \quad (A.18)$$

where $\mu = b - c^2/(a+1)$ is the symplectic eigenvalue of covariance matrix γ_B.

By making suitable replacements in the above formulas we can straightforwardly calculate also χ_{BE} and the mutual information and Holevo quantity for protocol including noiseless amplification or noiseless attenuation.